

Security & Best Practices

In doing the edTPA, it is expected that you will follow all professional and ethical guidelines that go along with handling video data for student minors.

The scope of your professional responsibility will be covered by the permission forms that the school district uses, and at a very basic level these permission forms legally obligate you to act in a manner that best protects the privacy and identity of your students.

This document will introduce you to FERPA resources, and help you to understand the types of things you can and should do with your video data to maximally ensure your good faith compliance with your professional, ethical, and legal obligations.

More than with any other area of concern with the edTPA, if you have questions about any of the content here, then you should consult a faculty member for information about what you can and cannot do with your video data.

FERPA & Why Good Security is Important

FERPA is the Family Educational Rights and Privacy Act. This is the federal policy that governs the work you will be doing with respect to video recording minors, and sets regulations for compliance, and consequences for failure to meet those regulations. This is the reason you and everyone else signs a lot of forms. Last year FERPA breaches ran about \$200 per breach - messing up here with a class of 30 can run you \$6000, and risk immediate dismissal from your program.

Your best protection is a healthy amount of fear and a solid dedication to best practices.

Keep in mind that the things you do will have consequences. The best you can do for yourself is adhering to the best practices covered in the next section, and if you have questions about what to do with your video, then ask before doing anything.

For more information on the Family Educational Rights and Privacy Act visit:

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>



Six Best Practices

1. Don't share
 2. Password Protect Hardware
 3. Physically Protect
 4. Encrypt Data
 5. Backup
 6. Clean Devices
-

Don't share data

The first practice is **Don't Share**. Don't show the video or documents to anyone unless we specifically say that you can! Your edTPA videos should be shared with no one except yourself, your supervisor, and Pearson. Even if you happen to record the funniest thing you have ever seen, it needs to be for only you to see. This also extends to talking about the things that happen in or during your recording segment.

Password protect devices

The next best practice is to **Password Protect** your devices. This means anything that is going to be handling the video: the phone you record your segment with, the computer that you use to cut your clips down. **EVERYTHING** needs to be password protected. Passwords should be

secure, and they should be your own. If someone else knows the password for something you will have your videos on, then that is a liability. And again, DON'T SHARE!

Physically protect devices

You should also **Physically Protect** your Hardware. Not everything can be password protected. For those devices, as well as for those that can be password protected, it is important not to leave them unattended or in the open where someone can steal them.

***Even if someone else were to take your data and make it available,
you would still be the responsible party.***

Encrypt your data (OPTIONAL)

Another way to secure your data is by **Encryption**. Data encryption is a method of disguising your data – it makes it so that even if someone got ahold of your computer or a flash drive that had the video data, they wouldn't be able to see that data without having a password to decrypt it. We do strongly recommend that you have a flash drive to backup your data, but if you are using one, just be sure to encrypt it. If this is something you are interested in, the Campus IT HelpDesk can help you set that up. Campus IT information is given below.

NOTE: Encryption is not mandatory because doing this can be technically complex, and runs the risk of making your data inaccessible to even you - but if you know how to do this, and are comfortable with it, then you should.

UWO HelpDesk

Phone: 920-424-3020

Location: Demsey Building Room 207

Make backups of your data

Make sure you are **backing up your data**.

With all of the work entailed by the best practices so far you might think that it would be easiest to keep everything in one place, but then you set yourself up for a catastrophic data loss. The

video recording events you will be completing for the edTPA are one-time events. If you were to lose all of your video data, then you would need to redo the entire edTPA around whatever new teaching event you could arrange, which could mean waiting another semester.

Common backup tools include flash drives, Titan File or an external hard drive.

Delete files from devices that aren't yours

Finally, **clean your devices**. After recording, make sure you move your files and data from less secure to more secure devices and then delete them from the original device. Make sure you are cleaning your devices, especially if you are borrowing them from the library. Just because it's a school device doesn't protect you.